Attributes on Smart Cards
Efficient Selective Disclosure with Idemix
&
IRMA: I Reveal My Attributes

Pim Vullers

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

Trans Link Systems - Wetenschapsforum
25th March 2013
Privacy issues

- Smart cards are “Big Brother’s little helper” (Stefan Brands)
- With OV-chipcard / Oyster / Charlie / . . . , you tell who you are when you get on a bus, metro, train, . . .
- Identity-based solutions violate their users’ privacy (and increase identity-fraud risk)

Attribute-based credentials

- Attribute-based authorisation: only provide the information which the system needs
- Example of attribute-based credentials (electronic wietpas):
  - card only says “I’m a Dutch citizen, and my age is above 18”
Outline

Introduction

Idemix Credentials

Results

IRMA – I Reveal My Attributes
Credentia-based System

The ideas

- Attributes
- Selective disclosure / Data minimisation
- Zero-knowledge / Randomisation

Idemix credential

- Attributes
- Master secret
- Issuer’s signature
Uses of a Credential

1 **Issuance**
   - *Blind issuing* of a credential
   - Issuer unlinkability

2 **Presentation**
   - *Selective disclosure* of the credential’s attributes
   - Randomisation of the Issuer’s signature

3 **Verification**
   - *Zero-knowledge proof* using the Issuer’s public key
   - Multi-show unlinkability
Uses of a Credential

1. **Issuance**
   - *Blind issuing* of a credential
   - Issuer unlinkability

2. **Presentation**
   - *Selective disclosure* of the credential’s attributes
   - Randomisation of the Issuer’s signature

3. **Verification**
   - *Zero-knowledge proof* using the Issuer’s public key
   - Multi-show unlinkability
Uses of a Credential

1 Issuance
   - Blind issuing of a credential
   - Issuer unlinkability

2 Presentation
   - Selective disclosure of the credential’s attributes
   - Randomisation of the Issuer’s signature

3 Verification
   - Zero-knowledge proof using the Issuer’s public key
   - Multi-show unlinkability
Design of the System

- CardService translates Idemix commands and data types into APDU commands for smart card communication
- MULTOS implementation, limited by smart card characteristics, is 95% compatible with Idemix Library

![Diagram showing the interaction between Idemix CardService, IBM's Idemix Library, and MULTOS card with Idemix application.]
Introduction

Idemix Credentials

Results

IRMA – I Reveal My Attributes
Related Work on Smart Cards

Related work

• Bichsel et al. (IBM Research, 2009), ± 7.5 sec
  Camenisch & Lysyanskaya anonymous credential system

• Sterckx et al. (KU Leuven, 2009), ± 3 sec
  Direct anonymous attestation

Our previous results

• Batina et al. (RU Nijmegen, 2010), ± 1.5 sec
  Self-blindable certificates of Verheul

• Hoepman et al. (RU Nijmegen, 2010), ± 0.6 sec
  Optimised self-blindable certificates

• Mostowski and Vullers (RU, 2011), ± 0.5 - 0.9 sec
  U-Prove selective disclosure (2-5 attributes)
Figure: Credential issuance times (□: computation, □: overhead).
Presentation Performance

Figure: Attribute verification times (black: computation, gray: overhead).
Conclusion

- Efficient MULTOS implementation of the Idemix technology
- Multi-show unlinkability of the credentials on the smart card
- Attribute-base credentials on smart cards are possible
- Major improvement over IBM’s DAA implementation

Next steps:
- Studying other technologies
- Practicing with other platforms
- Making anonymous credentials usable
IRMA

I reveal my attributes
1. **Pilot project**
   - Kerckhoffs students will receive an IRMA card
   - Online credential issuance, free printing, discount on coffee

2. **Proof-of-Concept**
   - Project for the government
   - MijnOverheid integration, POS-terminal integration

**Project partners:**

- Radboud University Nijmegen
- novay
- TNO
- SURFnet
- SIDN
Acknowledgements: the people behind IRMA

- Gergely Alpár
- Maarten Everts (TNO)
- Hans Harmannij
- Jaap Henk Hoepman (RU & TNO)
- Bart Jacobs
- Wouter Lueks (RU & TNO)
- Martijn Oostdijk (Novay)
- Roland van Rijswijk (RU & SurfNet)
- Peter Schwabe
- Pim Vullers
- Ronny Wichers Schreur
Questions